Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

Claim 1 (Currently amended): Method for cryptographically processing data, comprising:

a) feeding, to a cryptographic process (P), values, namely, the data (X) and a key (K), ~~and~~

b) carrying out the process (P) in order to form cryptographically processed output data (Y), characterized by

c) feeding, to the process (P), auxiliary values that mask the data (X) used in the process (P), ~~(K*; A, B)~~ and

d) compensating, by an auxiliary process, the influence of the auxiliary values ~~to~~on the output data (Y).

~~, in order to mask the values (K; D) used in the process (P).~~

Claim 2 (Currently amended): ~~Method according to claim 1, wherein an auxiliary value comprises a supplementary key (K*) which is fed to a supplementary process (P*) in order to form the key (K).~~ Method for cryptographically processing data, comprising;

a) feeding, to a cryptographic process (P), values, namely data (X) and a key (K),

b) carrying out the process (P) in order to form cryptographically processed output data (Y), characterized by

c) feeding, to a supplementary process (P*), a supplementary key (K*) in order to form the key (K),

d) wherein the supplementary key (K*) masks the key (K) used in the process (P), and

e) wherein the supplementary process (P*) comprises a cryptographic process to which an auxiliary key (K') is fed.

Claim 3 (Cancelled).

Claim 4 (Previously presented): Method according to claim 2, wherein the supplementary process (P*) is an invertible process.

Claim 5 (Previously presented): Method according to claim 2, wherein the data (X) is also fed to the supplementary process (P*).

Claim 6 (Original): Method according to claim 5, wherein carrying out the supplementary process (P*) takes place exclusively if the data (X) has predetermined properties.

Claim 7 (Previously presented): Method according to claim 2, wherein the process (P) and the supplementary process (P*) each are built up from a number of steps, and wherein steps of the process (P) and the supplementary process (P*) are alternated.

Claim 8 (Currently amended): Method according to claim 1, wherein the process (P) comprises a number of steps (S_i), each having a cryptographic operation ~~(F_i, F_i', F_i'')~~ for processing right-hand data (RD_i) derived from the data (X) and a combinatory operation (C_i) for combining with left-hand data (LD_i) also derived from the data (X), the processed right-hand data (FD_i) in order to form modified left data (SD_i), and wherein the right-hand data (RD_i) is combined with a primary auxiliary value (A_1) prior to the first step(S_1) and the left-hand data(LD_1) is combined with an additional auxiliary value (A_0).

Claim 9 (Original): Method according to claim 8 wherein, immediately after the last step (S_n), the right-hand data (RD_n) is combined with a further primary auxiliary value (A_n) and the modified left-hand data (SD_n') is combined with a further additional auxiliary value (A_{n+1}).

Claim 10 (Currently amended): Method according to claim 8, wherein the right-hand data (RD_i) is combined, in each step (S_i) and prior to ~~the~~ a cryptographic operation (F_i'), with the primary auxiliary value (A_i) of said step (S_i).

Claim 11 (Currently amended): Method according to claim 10, wherein the processed right-hand data (FD_i) is combined, following ~~the~~ a cryptographic operation (F_i), with the secondary auxiliary value (B_i) of said step (S_i).

Claim 12 (Original): Method according to claim 11, wherein the secondary auxiliary value (B_i) of a step (S_i) is formed

from the combination of the primary auxiliary value (A_{i-1}) of the preceding step and the primary auxiliary value (A_{i+1}) of the next step.

Claim 13 (Previously presented): Method according to claim 8, wherein all primary auxiliary values (A_i) are equal.

Claim 14 (Currently amended): Method according to claim 9, wherein the 25 primary auxiliary values (A_i) and/or secondary auxiliary values (B_i) have each time been combined with ~~the~~ a respective cryptographic operation (F_i) in advance.

Claim 15 (Currently amended): Method according to claim 14, wherein a combined cryptographic operation (F_i') contains several tables, and wherein the tables are determined in a different order each time the process (P) is carried out.

Claim 16 (Currently amended): Method according to claim 14, wherein a combined cryptographic operation (F_i') contains several tables, and wherein the elements of the tables are determined and/or stored in a different order each time the process (P) is carried out.

Claim 17 (Original): Method according to claim 16, wherein the order is stored as a lookup table for the benefit of reading out the elements.

Claim 18 (Previously presented): Method according to claim 8, wherein the right-hand data (RD_i) is combined with a tertiary auxiliary value (W_i) after each step (S_i).

Claim 19 (Original): Method according to claim 18, wherein the tertiary auxiliary value (W_i) in all steps, except the last one (S_n) is equal to the combination of the primary auxiliary value (A_1) of the first step (S_1) and the additional auxiliary value (A_0), and in the last step (S_n) is equal to zero.

Claim 20 (Previously presented): Method according to claim 8, wherein combining is carried out using an XOR operation.

Claim 21 (Previously presented): Method according to claim 1, wherein the data (X) comprises identification data of a payment means (1) and the processed data (Y) forms a diversified key.

Claim 22 (Currently amended): Method according to claim 1, wherein the process (P) comprises DES.~~, preferably triple DES.~~

Claim 23 (Previously presented): Circuit (10) for carrying out the method according to claim 1.

Claim 24 (Original): Payment card (1), provided with a circuit (10) according to claim 23.

Claim 25 (Original): Payment terminal (2) provided with a circuit (10) according to claim 23.

Claim 26 (New): Method according to claim 2, wherein the data (X) comprises identification data of a payment means (1) and the processed data (Y) forms a diversified key.

Claim 27 (New): Method according to claim 2, wherein the process (P) comprises DES.

Claim 28 (New): Circuit (10) for carrying out the method according to claim 2.

Claim 29 (New): Payment card (1), provided with a circuit (10) according to claim 28.

Claim 30 (New): Payment terminal (2) provided with a circuit (10) according to claim 28.

Claim 31 (New): Method according to claim 22, wherein the DES process is triple DES.

Claim 32 (New): Method according to claim 27, wherein the DES process is triple DES.